

# **EXHIBIT A**

COPY

MATTHEW RIGHETTI (SBN: 121012)  
matt@righettilaw.com

**RIGHETTI GLUGOSKI, P.C.**

The Presidio of San Francisco

220 Halleck Street, Suite 220

San Francisco, CA 94129

Tel: (415) 983-0900

Fax: (415) 397-9005

Attorneys for Plaintiff and the Proposed Class

FILED

JUN 18 2021

JAMES M. KIM, Court Executive Officer  
MARIN COUNTY SUPERIOR COURT  
By: L. Perdigao, Deputy

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
MARIN COUNTY**

AMY WYNNE, individually, and on behalf  
of a class of similarly situated persons,

Plaintiff,

v.

AUDI OF AMERICA, and DOES 1-50  
inclusive,

Defendants.

Case No. **CIV 2102450**

CLASS ACTION

**COMPLAINT FOR:**

**(1) NEGLIGENCE**

**(2) VIOLATION OF CALIFORNIA'S  
UNFAIR COMPETITION LAW (Bus.  
& Prof. Code, § 17200)**

DEMAND FOR JURY TRIAL

Plaintiff Amy Wynne brings this lawsuit against Audi of America on behalf of herself and all others similarly situated ("Class" or "Class Members") for violation of their privacy rights. Plaintiff alleges, upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

**NATURE OF THE ACTION**

1. Audi of America is the business of selling, leasing and repairing automobiles. Since at least 2014, Audi of America employed a vendor to market to buyers and interested buyers. (Audi of America and its vendor are collectively referred herein as "Defendant" or

1 “Audi.”) Audi was entrusted with personal identifiable information (“PII”)<sup>1</sup> of Audi customers  
2 and potential customers (collectively, “Customers”).

3 2. Between August 2019 and May 2021, Audi was the target of a massive data  
4 breach in which approximately 3.3 million Customers were subject to an unauthorized access  
5 and exfiltration, theft, or disclosure of their PII (“Data Breach”). Outside parties accessed a  
6 trove of personal details about Defendant’s Customers—such as names, home and business  
7 addresses, emails addresses, driver’s license numbers, social security numbers, and other  
8 information – stored on one of Audi’s servers. Audi maintained the highly sensitive PII in a  
9 form that was neither encrypted nor redacted.

10 3. In addition to violating the fundamental privacy rights of Plaintiff and Class  
11 Members, the Data Breach has caused them to suffer ongoing economic damages and other  
12 actual damages. Because of the Data Breach, they face an increased risk of identity theft and  
13 concomitant expenses associated with mitigating that risk. Plaintiff and Class Members require  
14 robust credit monitoring services and software to reasonably mitigate the danger of future  
15 identity theft and fraud.

16 4. Plaintiff brings this lawsuit on behalf of Class Members whose PII was  
17 compromised as a result of the Data Breach and Audi’s failure to (i) implement and maintain  
18 reasonable security procedures and practices appropriate to the nature of the PII; (ii) disclose  
19 its inadequate security procedures and practices; (iii) effectively monitor its systems for  
20 security vulnerabilities; and (iv) failure to timely detect, report, and disclose the Data Breach.

21 5. Audi’s conduct, as alleged herein, was negligent, constitutes an unfair business  
22 practice under California’s Unfair Competition Law (Bus. & Prof. Code, § 17200) (“UCL”).

## 23 II. PARTIES

24 6. At all relevant times, Plaintiff Amy Wynne was and is a citizen of California,  
25 residing in Marin County. Wynne is a customer of Audi. She entrusted her PII to Audi.

---

26  
27 <sup>1</sup> As used herein, the term “PII” is intended to include the definition of personal  
28 information provided under Civil Code sections 1798.140, subdivision (o), and 1798.81.5,  
subdivision(d)(1).

1 Wynne's PII was accessed and compromised as a result of the Data Breach. This resulted in an  
2 invasion of her privacy interests, loss of value of his PII, and has placed her at imminent,  
3 immediate, and continuing risk of further identity theft-related harm. Wynne has spent money  
4 on a credit monitoring service as part of a reasonable effort to mitigate against such harm and  
5 will continue to incur such expenses on an ongoing basis.

6 7. Defendant Audi of America is an entity doing business in California. Plaintiff is  
7 informed and believes and thereon alleges that Audi of America is a division of Audi AG  
8 which is a wholly owned subsidiary of Volkswagen Group. Audi of America is headquartered  
9 in Herndon, Virginia.

10 8. Plaintiff does not know the true names and capacities of Defendants sued  
11 herein as Does 1 through 50, inclusive, and therefore sues these defendants by such fictitious  
12 names. Plaintiff is informed and believes that each of the Doe Defendants was in some manner  
13 legally responsible for the damages alleged below. Plaintiff will amend this Complaint to set  
14 forth the true names and capacities of these Defendants when ascertained, along with  
15 appropriate charging allegations.

16 9. Plaintiff is informed and believe, and thereupon allege, that each of Defendants  
17 designated herein as a Doe is responsible in some actionable manner for the events and  
18 happenings referred to herein, and caused injuries to Plaintiffs, as hereinafter alleged, either  
19 through said Defendants' conduct, or through the conduct of their agents, servants, employees.  
20 The term "Defendant(s)" as used in this Complaint includes both the named Defendant and  
21 Defendants sued under the fictitious names of Does 1 through 50, inclusive.

22 10. Plaintiff is informed and believes and therefore alleges that, at all times relevant  
23 to this action, Defendants, and each of them, were the agents, servants, employees, assistants,  
24 and consultants of each of their co-Defendants, and were, as such, acting within the course of  
25 and scope of the authority of their agency and employment, and that each and every Defendant  
26 when acting as a principal, was negligent and careless in the selection and hiring of each and  
27 every co-Defendant as an agent, servant, employee, assistant and/or consultant.

### 28 **III. JURISDICTION AND VENUE**



1 number; (5) social security number; (6) date of birth; (7) account and loan numbers; and (8) tax  
2 identification number.

3 19. The Data Breach subjected Plaintiff and the other Class Members to an  
4 unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted  
5 PII, including, but not limited to, PII that falls within the definition of subparagraph (A) of  
6 paragraph (1) of subdivision (d) of Civil Code section 1798.81.5.

7 20. The Data Breach resulted from Audi's violation of the duty to implement and  
8 maintain reasonable security procedures and practices appropriate to the nature of the PII.  
9 On information and belief, Audi breached its standard of care by failing to implement  
10 reasonable security procedures to adequately protect Class Members' PII—which was not  
11 password protected, redacted, or encrypted—from data breaches. Data breaches, such as this  
12 one, are commonly made possible through a vulnerability in a system or server.

13 21. As a result of Audi's lax security, outside parties have accessed Plaintiff's and  
14 Class Members' PII in a readily usable form that is potentially of great value to them. Plaintiff  
15 and Class Members are thus exposed to criminals seeking to use the PII for nefarious and  
16 illegal activities, such as identity theft schemes. Given the sensitive nature of the PII, Plaintiff  
17 and Class Members face an immediate, concrete, and ongoing risk of identity theft.

18 22. At all relevant times, Audi knew, or reasonably should have known, of the  
19 importance of safeguarding PII and of the foreseeable consequences that would occur if its data  
20 security system was breached, including the significant costs, damages and harm that would be  
21 imposed on Plaintiff and the Class.

22 23. Over the past several years, large data breaches, such as the one that occurred  
23 here, have garnered widespread media attention and have been the focus of protective  
24 legislation and scrutiny by law enforcement and the media. Ignoring the known risk, Audi's  
25 approach to maintaining the security of the PII of Plaintiff and Class Members was well-below  
26 the standard of care.

27 24. As a result of the Data Breach, Plaintiff and Class Members now face years of  
28 constant surveillance of their financial and personal records, monitoring, and loss of rights.

1 Plaintiff and the Class are also subject to a higher risk of phishing and pharming, where  
 2 hackers exploit information they have already obtained in an effort to procure even more PII.  
 3 Moreover, Plaintiff and the Class now run the risk of unauthorized individuals creating credit  
 4 cards in their names, taking out loans in their names, and engaging in other fraudulent conduct  
 5 using their identities. Further, Plaintiff and Class Members have experienced a loss of value of  
 6 their PII as a result of the Data Breach. Given that Class Members are currently at risk of  
 7 identity theft or credit fraud, prophylactic measures, such as the purchase of credit monitoring  
 8 services and software, are reasonable and necessary to prevent and mitigate future loss.

9 ***California Recognizes the Importance of Protecting PII***

10 25. The CCPA affords California residents security protections and rights to learn  
 11 about and control how a business handles their personal information. The Legislature requires  
 12 businesses to implement adequate standards to protect PII:

13 It is the intent of the Legislature to ensure that personal information about  
 14 California residents is protected. To that end, the purpose of this section is to  
 15 encourage businesses that own, license, or maintain personal information about  
 16 Californians to provide reasonable security for that information.

17 (Civ. Code, § 1798.81.5, subd. (a)(1).)

18 26. The CCPA further endows on California residents the right to bring an action  
 19 for statutory damages if their information is subject to a data breach that is “a result of the  
 20 business’s violation of the duty to implement and maintain reasonable security procedures and  
 21 practices appropriate to the nature of the information.” (Civil Code, § 1798.150.)

22 ***PII Is Valuable to Hackers and Thieves***

23 27. Hackers and criminals recognize the value of PII. Identity thieves use stolen PII  
 24 for a variety of crimes, including credit card fraud, phone or utilities fraud, and financial fraud.  
 25 PII can also be sold on the dark web or used to clone a credit card.

26 28. Once hackers obtain access to PII, it can then be used to gain access to different  
 27 areas of the victim’s digital life, including bank accounts, social media, and credit card details.  
 28 Other sensitive data may be harvested from the victim’s accounts, as well as from those



1 belonging to family and friends.

2       29. Access to PII provides criminals further opportunity to hack into email  
3 accounts. Since most online accounts require an email address, not only as a username but also  
4 to verify accounts and reset passwords, a hacked email account can provide access to  
5 additional identity theft opportunities.

6       30. Hacked PII also allows thieves to obtain other personal information through  
7 “phishing.” According to the Report on Phishing available on the United States, Department  
8 of Justice’s website: “AT&T, a large telecommunications company, had its sales system  
9 hacked into, resulting in stolen order information including full names and home addresses,  
10 order numbers, and credit card numbers. The hackers then sent each customer a highly  
11 personalized e-mail indicating that there had been a problem processing their order and re-  
12 directing them to a spoofed website where they were prompted to enter further  
13 information, including birthdates and Social Security numbers.”<sup>2</sup>

14       31. Industry experts have reported that one in every three people who is notified of  
15 being a potential fraud victim becomes one. In the case of a data breach, simply reimbursing a  
16 consumer for a financial loss due to identity theft and fraud does not necessarily make that  
17 individual whole. The Department of Justice’s Bureau of Justice Statistics (“BJS”) has found,  
18 “among victims who had personal information used for fraudulent purposes” a significant  
19 percentage of victims spent a month or more resolving problems, with some even taking more  
20 than year.<sup>3</sup>

21       32. A person whose PII has been obtained and compromised may not know or  
22 experience the full extent of identity theft or fraud for years. In addition, a victim may not  
23 become aware of fraudulent charges when they are nominal because typical fraud-prevention  
24

---

25       <sup>2</sup> [https://www.justice.gov/archive/opa/docs/report\\_on\\_phishing.pdf](https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf) (accessed on August  
26 24, 2020).

27       <sup>3</sup> “Victims of Identity Theft,” U.S. Department of Justice, Dec 2013, available at  
28 <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (accessed on August 24, 2020).



1 algorithms fail to capture such charges. Those charges may be repeated, over and over,  
2 without detection.

3 ***Annual Monetary Losses from Identity Theft are in the Billions of Dollars***

4 33. Losses from identity theft reached \$21 billion in 2013. (See 2013 Javelin  
5 Strategies Identity Fraud Report.) According to the BJS, an estimated 17.6 million people  
6 were victims of one or more incidents of identity theft in 2014.

7 34. There often can be a time lag between the theft of PII and when the harm  
8 occurs or is discovered. According to the U.S. Government Accountability Office (“GAO”),  
9 which conducted a study regarding data breaches:

10 [L]aw enforcement officials told us that in some cases, stolen data may be held for  
11 up to a year or more before being used to commit identity theft. Further, once  
12 stolen data have been sold or posted on the Web, fraudulent use of that information  
13 may continue for years. As a result, studies that attempt to measure the harm  
14 resulting from data breaches cannot necessarily rule out all future harm.<sup>4</sup>

15 ***Plaintiff and Class Members Have Suffered Ongoing Damages***

16 35. As a direct and proximate result of the Data Breach caused by Audi’s wrongful  
17 actions and inaction, Plaintiff and Class Members have been placed at an imminent and  
18 continuing risk of harm from identity theft and identity fraud, requiring them to take the time  
19 and effort to mitigate any actual or potential impact of the Data Breach. Plaintiff and Class  
20 Members now must reasonably incur the ongoing expense of surveilling their financial and  
21 personal records and monitoring. They are subject to a higher risk of phishing and  
22 pharming schemes, through which hackers exploit the ill-gotten PII to procure additional  
23 private information. In addition, Plaintiff and Class Members run the risk of unauthorized  
24 individuals creating credit cards in their names, taking out loans in their names, and engaging  
25 in other fraudulent conduct using their identities.

26 36. The Data Breach has caused Plaintiff and Class Members to suffer ongoing

27  
28 <sup>4</sup> See GAO, Report to Congressional Requesters, at 33 (June 2007), available at  
<http://www.gao.gov/new.items/d07737.pdf> (accessed on August 24, 2020).

1 economic damages and other actual harm for which they are entitled to compensation,  
2 including, but not limited to, the following:

- 3 (i) lost or diminished value of PII;
- 4 (ii) out-of-pocket expenses associated with the prevention, detection, and recovery  
5 from identity theft, tax fraud, and/or unauthorized use of their PII;
- 6 (iii) lost opportunity costs associated with attempting to mitigate the actual  
7 consequences of the data breach;
- 8 (iv) deprivation of rights under the UCL and CCPA; and
- 9 (v) an increased risk to their PII, which has been compromised and thus (a) is  
10 subject to criminal access and abuse; and (b) remains in Audi's possession and  
11 is subject to further unauthorized disclosures so long as Audi fails to undertake  
12 appropriate and adequate measures to protect the PII.

### 13 V. CLASS ALLEGATIONS

14 37. Plaintiff bring this action on their own behalf and on behalf of a class of  
15 individuals pursuant to CCP 382. Plaintiff intends to seek certification of a class defined as  
16 follows:

17 **All Audi of America's customers and interested buyers residing in**  
18 **California whose PII was accessed or otherwise compromised in the**  
19 **Data Breach, which, according to the Notice of Data Breach provided by**  
20 **Audi of America, occurred at some point between August 2019 and May**  
21 **2021.**

22 Excluded from the Class are the following individuals and/or entities: Defendant and its  
23 parents, subsidiaries, affiliates, officers and directors, current or former employees, and  
24 any entity in which Defendant has a controlling interest and all individuals who make a  
25 timely election to be excluded from this proceeding using the correct protocol for opting  
26 out.

27 38. **Numerosity.** The members of the Class are so numerous that joinder of all Class  
28 Members is impractical. While the exact number of Class Members is unknown to Plaintiff at

1 this time, Defendant's Notice of Data Breach states that approximately 3.3 million individuals  
 2 are involved. It is unknown at this time how many of those 3.3 million individuals are  
 3 California residents but, on information and belief, Plaintiff alleges that the number of Class  
 4 Members is at least in the tens of thousands. Class Members are readily identifiable from  
 5 information and records maintained by Audi.

6       39.     **Commonality and Predominance.** This action involves questions of law and  
 7 fact common to Class Members that predominate over any questions affecting individual Class  
 8 Members. These common questions of law and fact include, without limitation:

- 9           a. When Audi actually learned of the Data Breach;
- 10          b. Whether Audi adequately detected, disclosed and responded to the Data  
 11 Breach;
- 12          c. Whether Audi owed a duty to the Class to exercise due care in collecting,  
 13 encrypting, password protecting, storing, safeguarding and/or maintaining  
 14 their PII;
- 15          d. Whether Audi implemented and maintained reasonable security procedures  
 16 and practices appropriate to the nature of the PII;
- 17          e. Whether Audi breached its duty of care;
- 18          f. Whether Audi knew or should have known that they did not employ  
 19 reasonable measures to keep Plaintiff's and Class Members' PII secure and  
 20 prevent loss or misuse of that PII;
- 21          g. Whether Audi adequately addressed and fixed the vulnerabilities that  
 22 permitted the Data Breach to occur;
- 23          h. Whether Audi caused Plaintiff and Class Members to incur damages;
- 24          i. Whether Audi violated the law by failing to promptly notify Class Members  
 25 that their PII had been compromised;
- 26          j. Whether Plaintiff and the other Class Members are entitled to credit  
 27 monitoring and other monetary relief;
- 28          k. Whether Defendant violated California's UCL by failing to implement

1 reasonable security procedures and practices;

- 2 1. Whether Class Members are entitled to statutory damages, special or general  
3 damages, civil penalties and/or injunctive relief; and

4 40. **Typicality:** Plaintiff's claims are typical of those of other Class Members  
5 because all had their PII accessed and compromised as a result of the Data Breach, due to  
6 Audi's wrongful conduct, acts, or omissions.

7 41. **Adequacy:** Plaintiff's interests are not antagonistic and do not irreconcilably  
8 conflict with the interests of the Class. Plaintiff is represented by attorneys who are competent  
9 and experienced in consumer and privacy-related class action litigation.

10 42. **Superiority and Manageability:** A class action is superior to other available  
11 group-wide methods for the fair and efficient adjudication of this controversy because the  
12 individual damage and harm suffered by each individual Class Member may be relatively small  
13 compared to the expense and burden of prosecuting such an individual case, and the difficulty  
14 of discovering and remedying the wrongdoing of Audi. If individual Class Members were  
15 required to bring separate actions, courts would be confronted by a multiplicity of lawsuits  
16 burdening the court system while also creating the risk of inconsistent rulings and  
17 contradictory judgments. In contrast to proceeding on a case by case basis, in which  
18 inconsistent results will magnify the delay and expense to all parties and the court system, this  
19 class action presents far fewer management difficulties while providing unitary adjudication,  
20 economies of scale and comprehensive supervision by a single court.

21 43. Audi has acted on grounds generally applicable to the entire Class, thereby  
22 making final injunctive relief and/or declaratory relief appropriate with respect to the Class as a  
23 whole.

24 44. Likewise, certain issues are appropriate for certification because such claims  
25 present only particular, common issues, the resolution of which would advance the disposition  
26 of this matter and the parties' interests therein. Such issues include, but are not limited to:

- 27 a. Whether Audi owed a legal duty to Plaintiff and the Class Members to  
28 exercise due care in collecting, storing, using, and safeguarding their PII;

- b. Whether Audi breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Audi failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Audi has failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
- e. Whether Class Members are entitled to actual damages, statutory damages, credit monitoring or other injunctive relief, as a result of Audi's wrongful conduct.

45. Notice of the pendency of and any resolution of this action can be provided to the Class members by individual mailed notice or the best notice practicable under the circumstances.

#### **FIRST CAUSE OF ACTION**

[Negligence]

46. Plaintiff re-alleges herein the allegations contained in paragraphs 1 through 45, and allege against Defendant as follows.

47. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

48. The duties owed by Defendant to Plaintiff and Class Members include, but are not limited to, the following:

- a) To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class Members within its possession;
- b) To protect PII of Plaintiff and Class Members in its possession by using reasonable and adequate data security practices and procedures; and
- c) To implement practices and procedures to quickly detect and timely act on data breaches, including promptly notifying Plaintiff and Class Members of the data breach.

1           49. Defendant breached its duty owed to Plaintiff and Class Members. Defendant  
2 knew or should have known the risks of maintaining and storing PII and the importance of  
3 maintaining secure systems.

4           50. Defendant knew or should have known that its security procedures and practices  
5 did not adequately safeguard Plaintiff's and the other Class Members' PII. Defendant also  
6 failed to timely detect the Data Breach and failed to encrypt, redact, and password protect the  
7 Class Members' PII.

8           51. Through Defendant's acts and omissions described in this Complaint,  
9 Defendant failed to provide adequate security to protect the PII of Plaintiff and the Class from  
10 being accessed and compromised.

11           52. Defendant breached the duties it owed to Plaintiff and Class Members in several  
12 ways, including:

13               a) Failing to implement adequate and reasonable security systems,  
14 protocols, and practices sufficient to protect Class members' PII, creating a foreseeable risk of  
15 harm;

16               b) Failing to comply with the minimum industry security standards for data  
17 security;

18               c) Failing to act despite knowing or having reason to know that  
19 Defendants' systems were vulnerable to attacks; and

20               d) Failing to timely and accurately disclose to Plaintiff and Class Members  
21 that their PII was captured, accessed, exfiltrated, stolen, disclosed, viewed, and/or misused.

22           53. Due to Defendant's conduct, Plaintiff and Class Members require, among other  
23 things, extended credit monitoring. The Data Breach creates an increased risk for identity theft  
24 and other types of financial fraud against the Class members. The consequences of identity  
25 theft are serious and long-lasting. There is a benefit to early detection and monitoring.

26           54. As a result of Defendant's negligence, Plaintiff and Class Members suffered  
27 injuries and damages that include and/or may include: (i) the lost or diminished value of PII;  
28 (ii) out-of-pocket expenses associated with the prevention, detection, and/or recovery from

identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach; (iv) the continued risk to their PII, which can be subject to further unauthorized access and disclosure; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and/or repair the impact of the PII compromised as a result of the Data Breach, including ongoing credit monitoring.

55. These injuries, which also include an invasion of privacy rights, were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

### **SECOND CAUSE OF ACTION**

[Violation of California's Unfair Competition Law  
Cal. Bus. & Prof. Code §17200 – Unlawful Business Practices]

56. Plaintiff re-alleges herein the allegations contained in paragraphs 1 through 55, and allege against Defendant as follows.

57. Defendant has engaged and continue to engage in acts and practices of unfair competition, as that term is defined in Business & Professions Code section 17200, including unlawful, unfair or fraudulent business acts or practices.

58. Defendant engaged in unlawful acts and practices by failing to implement reasonable and adequate data security practices and procedures, as described herein, by obtaining Plaintiff's and Class members' PII with knowledge that the information would not be adequately protected; by storing Plaintiff's and Class members' PII in an unsecure electronic environment; and by failing to timely detect and report the Data Breach.

59. Defendant has violated Civil Code section 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII of Plaintiff and the Class Members.

60. Defendant also engaged in unlawful acts and practices, by failing to disclose the data breach, including to Class Members in a timely and accurate manner, which violates Civil Code section 1798.82. To date, Defendant has still not provided full and accurate information



1 regarding the Data Breach to Plaintiff and the Class Members.

2         61. Defendant's business practices are unfair under the UCL because it has acted in  
3 a manner that is unethical, oppressive, and/or substantially injurious to Plaintiff and the Class  
4 Members. The exposure of their PII to third parties is substantially injurious because of the  
5 significant harm that can result. The harmful impact of Defendant's practice far outweighs any  
6 possible countervailing benefits.

7         62. On information and belief, Defendant received money or property to protect PII,  
8 for the benefit of Plaintiff and the Class, but failed to implement adequate security policies and  
9 practices.

10         63. As a result of Defendant's unlawful, unfair, or fraudulent business practices as  
11 alleged herein, Plaintiff suffered injury in fact and lost money or property. Among other things,  
12 Plaintiff and Class Members are entitled to recover the price received by Defendant for the  
13 services described herein, the loss of Class Members' legally protected interest in the  
14 confidentiality and privacy of their PII, and additional losses as described above.

15         64. Defendant knew or should have known that its computer systems and data  
16 security practices and procedure were inadequate to safeguard Class members' PII and that the  
17 risk of a data breach or theft was likely.

18         65. Pursuant to Business & Professions Code §§ 17203 and 17204, the Court may  
19 enjoin such conduct in the future on behalf of the Class and the general public; obtain a  
20 provision for a corrective notice; and compel Defendant to restore to Plaintiff and Class  
21 Members any money or property that Defendant may have acquired or retained as a result of  
22 any act or practice that constitutes unfair competition. Plaintiff further seeks an order requiring  
23 Defendant to disgorge any profits Defendant may have obtained as a result of their conduct.

24         66. Plaintiff seeks restitution to Plaintiff and Class Members of money or property  
25 that Defendant may have acquired by means of its business practices alleged herein, including  
26 monetary restitution and restitutionary disgorgement of all profits accruing to Defendant  
27 because of such practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code  
28 Civ. Proc. § 1021.5), and injunctive or other equitable relief. Plaintiff and Class Members also

lost legally protected interest in the confidentiality and privacy of their PII, and suffered additional losses as described above.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of herself and all Class Members, request judgment against Audi and that the Court grant the following:


- A. An order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;
- B. An order enjoining Audi from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class Members' PII;
- C. An order instructing Defendant to purchase or provide funds for adequate credit monitoring services for Plaintiff and all Class Members;
- D. An award of compensatory and statutory damages, in an amount to be determined, including statutory damages pursuant to the CCPA;
- E. An award for equitable relief and restitution as a result of Audi's wrongful conduct;
- F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;
- G. Nominal damages; and
- H. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a jury trial of all issues so triable.

DATED: June 18, 2021

**RIGHETTI GLUGOSKI P.C.**

  
Matthew Righetti  
*Attorneys for Plaintiff*